© THE QUEEN'S PRINTER FOR ONTARIO
1999

REPRODUCED WITH PERMISSION

L'IMPRIMEUR DE LA REINE POUR L'ONTARIO

REPRODUIT AVEC PERMISSION

micromedia
a division of IHS Canada

20 Victoria Street
Toronto, Ontario M5C 2N8
Tel: (416) 362-5211
Toll free: 1-800-387-2689
Fax: (416) 362-6161
Email: info@micromedia.on.ca

Information
and Privacy
Commissioner/
Ontario

Biometrics and Policing:

Comments from a Privacy Perspective

Ann Cavoukian, Ph.D.
Commissioner
August 1999

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: http://www.ipc.on.ca

Table of Contents

1. Introduction 1
2. What is a Biometric? 2
   - 2.1 Definition 2
   - 2.2 How Biometrics are Used 2
   - 2.3 The Problem of Mismatching 3
   - 2.4 Different Types of Biometric Technologies 3
3. Applications of Biometric Technology 7
   - 3.1 Law Enforcement 7
   - 3.2 Banking 7
   - 3.3 Benefit Systems 8
   - 3.4 Computer/Network Security 8
   - 3.5 Immigration 8
   - 3.6 National Identity 8
   - 3.7 Physical Access 9
   - 3.8 Prisons and Correctional Facilities 9
   - 3.9 Telecommunications 9
   - 3.10 Employee Monitoring 9
4. Privacy Concerns 10
5. Biometrics as a Friend to Privacy 13
6. Possible Legal Limitations on the Use of Biometric Information 14
7. What Needs To Be Done To Make Partners of Biometrics and Privacy? 15
8. Conclusions 17
9. Appendix 18
10. Bibliography 21

1. Introduction

Biometrics and policing are not strangers to each other. Fingerprints have been used for the identification of suspects and victims for more than 100 years. Although crude in form, facial recognition through photographs and sketches à la the 'wanted' posters of the old West have been used for an even longer time. Today there are a large number of biometric systems being proposed for a staggering number of uses. Any organization dealing with issues of security, authentication and identification, will already have been deluged with offers to solve their problems through the use of a biometric system. While the benefits of their use are quite real, there are also certain aspects to the use of biometric systems that should raise some concerns. One of those concerns is privacy.

The purpose of this chapter is to provide some background and context to the use of biometrics and to make the reader aware of some of the issues surrounding their use. The purpose of the chapter is not to suggest that biometrics should not be used, but if used, they must be used responsibly. Biometric information is a part of ourselves and we would all wish that it be used conscientiously. Any technology has the ability to strike a balance between its benefits and its dangers. Because of the significant harm that could result from the misuse of biometrics, we must work hard at maintaining that balance. It is particularly important that any biometric system remain privacy neutral. In other words, the use of any biometric technology should not result in privacy being forfeited. Rather, the existing level of privacy should remain the same or, better still, be enhanced.

2. What is a Biometric?

2.1 Definition

A biometric is "a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity,"[1] — one of many definitions. The Biometrics Consortium is an organization that serves as the United States Government's focal point for research, development, testing, evaluation, and application of biometric-based personal identification/verification technology. The Consortium itself is in the midst of debating the definition, but currently holds that biometrics is "automatically recognizing a person using distinguishing traits."[2]

Those in the biometrics field argue strongly for the inclusion of other factors to clarify what a biometric is. How biometrics are used, whether the process is mechanical/automatic or whether the process is "non-physically invasive" are among the factors that some feel are important to incorporate into the definition. However for the purposes of this chapter, we will focus on the automatic, largely computer-based technologies based on physiological or behavioural characteristics or traits.

2.2 How Biometrics are Used

Biometric technologies are used almost exclusively for purposes of identification or authentication/verification. Identification is also often described as one-to-many matching. Automatic Fingerprint Identification Systems (AFIS) which match a single finger image against a database of images is one example. For the purposes of identification, a single biometric sample is compared to a collection of many other samples that can be linked to the sample owner's identity in the hopes that a match can be found. For authentication/verification, a single biometric sample is compared to a single sample (one-to-one) from a collection to verify or authenticate that the two samples have been obtained from the same individual.

For policing organizations, both uses of biometrics may be required. Authentication/verification is often part of the security procedures that an organization may use to control access or to monitor activities. Identification is an action that the lay person would associate most commonly with policing and the use of biometrics. Identifica-

[1] ICSA, Gary Roethenbaugh, ICSA Industry Analyst, *Biometrics Explained:* http://www.icsa.net/services/consortia/cbdc/explained.shtml

[2] Biometrics Consortium: http://www.biometrics.org/

tion is the more difficult of the two tasks that biometric technologies are used for — it is also the task most likely to have errors associated with its performance.

2.3 The Problem of Mismatching

The typical errors associated with the use of biometrics are 'false positive' matches and 'false negative' matches. Correct matches will result in either a true positive match (the "new" biometric sample matches with an "old" sample collected earlier from the same individual), or a true negative match (the "new" biometric sample is found to correctly have no match with a single sample collected earlier in the case of authentication/verification, or with any of the "old" samples in the case of identification).

When a false positive match occurs, the technology incorrectly identifies the "new" sample as a match for a specific "old" sample when that is not in fact the case. When a false negative occurs, the technology indicates there is no match between the "new" sample and a single sample collected earlier in the case of authentication/verification or with any of the "old" samples in the case of identification.

The error rates for various biometric technologies vary quite widely from technology to technology and can also vary quite widely as the circumstances of the sample collection vary. Matches between DNA samples are believed, in many circles, to be the most reliable but even here the courts have acknowledged there is some room for error, particularly if the collection and matching processes are compromised.

2.4 Different Types of Biometric Technologies

2.4.1 Body Odour

Each unique human smell is made up of chemicals knows as volatiles. These can be converted into a template by using sensors to capture body odour from non-intrusive parts of the body such as the back of the hand.

2.4.2 DNA

At present, use of DNA has largely been restricted to law enforcement activities involving one-to-one-matching. It is also, at present, relatively costly and time consuming to undertake. The additional information that can be gleaned from a DNA sample such as the presence of hereditary factors and medical disorders raises privacy concerns not associated with other biometric technologies.

The purportedly astronomical rate of accuracy and the infinitesimally small rates of false-negatives and false-positives puts DNA matching in a league by itself when compared to other biometric technologies. Although matching time is not yet reduced to the point of being sufficiently automatic for this method to be classified as a true biometric technology (the current best is 10 minutes), the use of DNA will be very attractive to developers of biometric systems when matching time is reduced.

Current processes for obtaining DNA samples are also quite intrusive, requiring some form of tissue, blood or other bodily sample. Although this also makes it presently unattractive as a biometric technology, alternative, less intrusive methods of obtaining samples are likely to be developed. Recently techniques have been developed that claim to be able to extract DNA from samples of hair or skin.[3]

2.4.3 Ear Shape

Ear shape markings have already been used in the law enforcement field but have not as yet been used for other applications.

2.4.4 Facial Recognition

Facial Recognition technologies involve complex processes, usually requiring sophisticated artificial intelligence and machine-learning techniques. There are a number of technologies in this area that use either video or thermal imaging to capture the sample. This technology mimics the way people recognize each other by using computer algorithms to simulate human interpretation of the face. The matching process can be affected by factors such as facial hair, glasses, aging or the position of the head. The technologies must be capable of adapting to these changes.

2.4.5 Finger Scanning

Perhaps the most widely used biometric technology is finger scanning (which is also very similar to palm scanning.) Finger scanning systems analyze tiny, unique features found on a fingerprint, known as 'minutiae.' These may be ridge endings, bifurcations (branches made by the ridges), sweat pores or the distance between ridges. Similar to the process of trained operator identification of fingerprints, the minutiae obtained from a new sample can then be compared on points of equivalence to an earlier, previously obtained sample.

[3] BBC News, New DNA weapon in fight against crime: http://news.bbc.co.uk/hi/english/sci/tech/newsid_287000/287777.stm

A number of factors affect the quality of the sample that is obtained. These can include age, gender; moisture, dirty, dry or cracked skin; ethnic background and pressure or alignment on the scanning device. Techniques for capturing an image include optical, thermal or tactile capacitance and ultra-sound.

2.4.6 Hand Geometry

In hand geometry, a three-dimensional image of the hand is taken and measures of the shape and length of fingers and knuckles are made. Finger geometry is similar but uses only individual fingers. In industry terms, this was one of the first biometric technologies developed. Both hand and finger geometry do not achieve the highest levels of accuracy but they are convenient and able to process large volumes of users quickly. Their predominant use is for access control.

2.4.7 Iris Recognition

Each person's iris has a unique and complexly patterned structure. The structure is a combination of specific characteristics called corona, crypts, filaments, freckles, pits, radial furrows and striations. Glasses affect the quality of the image obtained, but contact lens do not. Another reported advantage of iris recognition is that it is very unlikely that an artificial or dead iris could be used to fraudulently by-pass the system.

2.4.8 Keystroke

Also known as 'keystroke dynamics, keystroke biometrics analyze typing rhythm. Since keystroke dynamics are behavioural and evolve over time, technologies of this type must be able to continually check the identity of a person. Also, because it is behavioural, keystroke dynamics are affected by physical factors such as fatigue or distraction, which can affect accuracy.

2.4.9 Retinal Scan

The retina, the layer of blood vessels situated at the back of the eye, forms a unique pattern. Retinal biometrics are generally regarded as the most secure biometric method. A precise enrollment procedure is necessary, which involves lining up the eye to achieve an optimum reading. There are fears, although not fully investigated, that the intrusive process of shining light into the eye may cause some physical harm.

2.4.10 Personal Signature

This biometric technology is referred to as dynamic signature verification (DSV). It is the method of signing rather than the finished signature which is important and is not the same as the study of static signatures on paper (handwriting analysis.) A number of characteristics are examined by DSV including the angle at which the pen is held, the time taken to sign, the velocity and acceleration of the signature, the pressure exerted when holding the pen and the number of times the pen is lifted from the paper. An advantage of signature biometrics is the acceptance of a signature as a means of asserting identity and in a number of situations to legally bind an individual.

2.4.11 Vein Pattern

Vein pattern recognition analyzes the distinctive pattern of veins in the back of the hand that form when a fist shape is made by the hand. The vein structure, or "vein tree," is captured using infrared light.

2.4.12 Voice Recognition

Voice recognition biometrics focus on the sound of the voice. This is quite distinct from the technology that recognizes words and acts on commands. To avoid confusion, the terms "speaker recognition," "speaker verification" and "speaker identification" are used. Since the sound of a human voice is caused by resonance in the vocal tract, the length of the vocal tract and the shape of the mouth and nasal cavities affect the sound measured by this technology. The techniques for analyzing the voice may be captured with the user uttering a specifically designated password combining phrases, words or numbers, or with the user uttering any form of phrase words or numbers. Currently the former technique is most often used. This technology also has the advantage of being useful for telephone-based applications. However, environmental background noise and interference over telephone networks can affect the performance of these systems.

3. Applications of Biometric Technology

Although policing is primarily a law enforcement activity, those in the policing profession must have at least a working knowledge of a wide variety of other types of activities in order to become good at law enforcement. Biometrics are used in many areas other than law enforcement. To only consider the use of biometrics in the law enforcement realm would thus be limiting. Modern policing requires its practitioners to see beyond their realm in order to be truly effective.

3.1 Law Enforcement

The law enforcement area is probably the largest biometric user group. Primarily AFIS and palm-based technologies are used as an extension of traditional human processes. However, there have been applications based on other biometric technologies that are entering this area. As one example, United Kingdom authorities have tested the use of facial recognition to match images captured by surveillance cameras with a database of "criminals."

Law enforcement is coming to increasingly rely on the use of DNA-based technologies as an aid in solving crimes. Although not yet at the point of other biometric technologies in terms of speed, DNA matching cannot be ignored in this discussion. DNA is being used to process criminal suspects to separate the guilty from the innocent. It is also being used to identify victims and to match convicted offenders to outstanding crimes. To aid these processes, the establishment of DNA data banks is either underway or under consideration in several jurisdictions including Canada and the United States.

3.2 Banking

Fraud and breaches of security are of great concern to those in the banking industry. Identification/authentication for audit and transaction-tracking purposes is also a growing concern. Automated Banking machines (ABMs) and point of sale transactions are particular weak links that could easily be addressed by biometric technologies. Telephone and Internet banking also provide challenges in need of identification/ authentication. The difficulty of finding a technology that is generally acceptable to customers and that can become an industry standard remains. The vast expense of converting current systems presents an even greater obstacle.

3.3 Benefit Systems

Fraud is considered to be a significant problem for government benefit systems such as welfare or social assistance. Biometric technologies, particularly finger scanning, are seen to be one of the answers. The actual payment of benefits relates to one-to-one matching for authentication, while the enrollment stage involves a one-to-many match in order to eliminate "double dipping" or fraudulently obtaining multiple benefits by impersonating different identities. One example of an enrollment process is currently under development by the City of Toronto, Canada. Legislation passed in consultation with the Ontario Information and Privacy Commissioner contains legislated procedural and technical safeguards to protect the biometric information.

3.4 Computer/Network Security

Securing computers against unauthorized use, while far from being new, is an emerging area for the use of biometric technologies. Authentication to use a machine or computer systems is one aspect while another is verification for such activities as conducting commercial activity across the Net. The computing industry accumulates vast quantities of valuable information including banking data, business intelligence, credit card numbers, medical information and other personal data. This makes it an entity in need of special safeguards.

3.5 Immigration

Biometric technologies have found some of their earliest applications in the immigration area. The systems must quickly and efficiently process large numbers of travelers — separating the law-abiding travelers from the lawbreakers.

3.6 National Identity

Various nations around the world are adopting biometric technologies to assist in such activities as recording population growth, identifying citizens and preventing fraud in elections. Mexico, for example, has developed a more secure voter identification card complete with photograph and digitized fingerprint. Spain requires an identity card containing a digitized fingerprint. Colombia, in its Legislature, uses hand geometry to verify the identity of the country's legislators.

3.7 Physical Access

Physical access control is one of the broadest areas where biometric technologies are used. Initially used for high security areas such as nuclear power plants, military facilities and computing centres, the use of biometric systems has spread to schools, offices and supermarkets. The spread will undoubtedly continue to smaller areas such as houses and cars — it is expected that these systems will proliferate widely.

3.8 Prisons and Correctional Facilities

In the reverse of most physical access control systems, biometrics are used in prisons to keep people *in* rather than keep them out. Besides controlling physical movement within a prison or detention areas, biometric technologies are also being used to enforce home confinement orders and to regulate the movement of probationers and parolees.

3.9 Telecommunications

The rapid expansion of telecommunications systems has also made them a prime target for fraud. This fraud can take the form of "cloning" (obtaining a new telephone account using stolen code numbers), and new subscription fraud (obtaining a new phone account using a false identity). Also at risk is "Dial Inward System Access" which allows authorized individuals to contact a central exchange and make free calls. Voice recognition technologies are an obvious fit for this area.

3.10 Employee Monitoring

Employee attendance monitoring has historically been performed by "clocking-in and out" machines. Use of a biometric technology system not only prevents such abuses as someone else "punching-in" falsely for someone, but it can also be incorporated into the time management software to produce management accounting and personnel reports.

4. Privacy Concerns

The historic reaction to biometrics on the part of most privacy advocates is to view it as a threat to privacy. There are cultural objections raised where biometrics are seen as a loss of dignity, stigmatizing those from whom the biometric is collected. Religious objections may be raised. There are fears of physical invasiveness either directly in the case of DNA collection or retinal scan. Finally there are philosophical objections to the perceived loss of autonomy and control if the use of biometrics is so wide spread as to become virtually required to conduct the day-to-day aspects of one's life. But biometrics are also being put forward as a benefit to privacy by securely protecting one's identity and access to one's own information. As with all technologies, biometric technologies themselves are privacy neutral. It is how these technologies are used and how we set controls on their use that will answer the question — friend or foe?

A large part of the problem is similar to many new technologies — biometric technologies and their potential uses are simply not well understood. There is a great degree of mistrust associated with biometric technologies, partly because they at least seem to be invasive. Technologies that monitor people also lead to an increased feeling that there are fewer and fewer private spaces in which people can remain free from intrusions. Fingerprints have long been associated, particularly in Canada, with the exercise of power by the state over people, especially in relation to criminal law enforcement. The digitized finger scanning technologies now used in biometrics are easily confused with past ink-pad fingerprinting techniques, leading to a generalization of the negative perception associated with this practice. In other countries where wider ranges of organizations require the provision of fingerprints, the "criminal" stigma is not as prevalent.

Any high-integrity identifier such as a biometric can represent a threat to privacy because it represents the basis for a ubiquitous identification scheme. If there is a general reliance on biometric identification and authentication for a wide variety of daily transactions, our movements and behaviours could be efficiently tracked. Compilation of transactional information about a particular person that creates a picture of travels, preferences, affiliations or beliefs builds a detailed profile of that individual. Were that the case, we would not be able to go about our daily affairs with any degree of anonymity. Anonymity is seen by some as a benefit to illegal activities but there are many aspects of our affairs that many of us would legitimately prefer to keep to ourselves. Health problems, marital concerns, parental history or religious beliefs are features of ourselves that we may prefer not to be widely known. Tracking of citizens, surveillance societies and loss of autonomy are often associated in our minds with totalitarian governments but even well meaning regimes may use whatever

is in their control when they feel the end justifies the means. As an example, the governments of Canada and the United States felt justified in identifying and incarcerating those of Japanese ancestry during the Second World War. These people were at least, in part, identified through the use of census data. How much more efficiently could this have been accomplished with today's technologies and the myriad of available government databases?

It is this general encroachment that privacy advocates are most concerned about, often described as "function creep." There would be a great temptation to make use of such powerful databases because of the uniqueness of the information. The first applications of biometric technologies are for very limited, clearly specific and, for the most part, sensible purposes. Their use to combat increasing forms of fraud, improve airport security, or protect children would find few objectors. But, the greatest danger would be the expansion of such use for well-meaning purposes to others that went beyond the original purposes and failed to address the limitations of the original collection activity. The fear is that biometric systems could be used without notification for additional purposes not intended when the original system was implemented. And this fear would not be limited to government actions. The private sector is likely to have large biometric databases in the future. Uncontrolled matching of these databases with other databases, holding health insurance or credit information as examples, is viewed with great concern.

Most new technologies give off a perception of infallibility, particularly in the early stages of their development and use. This is particularly the case with biometric systems. The claims of their developers as to the individual uniqueness of their information suggest that they are vastly superior to current processes. However, with the exception of fingerprints, biometrics have not been sufficiently demonstrated to be unique to each individual. In fact DNA, in the case of identical twins, is by definition, not unique.[4] Even if the various biometrics can eventually demonstrate uniqueness, there exists the risk of false negatives and false positives as described above. If a criminal conviction is being sought and the decision hinges on information produced from a biometric system, we must be sure that the false negative and false positive rates of the system are known, and are accurate in practice, not just in theory.

An additional danger surrounding the reliability of biometric systems is not only their true reliability but also their perceived reliability. If the perception exists that they are irrefutable, then questioning them will become extremely difficult, not only in

[4] O'Connor, Sean, Collected, Tagged, and Archived: Legal Issues in the Burgeoning Use of Biometrics for Personal Identification: http://lummi.stanford.edu/class/law495/WWW/oconnor.htm.

the legal realm but also in the everyday realm. For example, records of entry to secure certain areas or identification provided for commercial transactions, will be virtually impossible to challenge. With today's reliance on computers as our record keepers, we are already faced with a desperate task to correct inaccuracies when our electronic identity is stolen. "The computer says" often becomes the final word. Theft of data, incorrect entry of data, "glitches" in the transfer of information are recognized as ways that errors are made, but imagine if the information was also tagged with a biometric. Would a claim that the information was in error be believed?

Of course, the irrefutability of such information would enormously increase its value for criminal activities. Nowadays, stealing the electronic identity of an individual by obtaining their credit card number, social benefits identification number or PINs and passwords provides the criminal with quick, easy and difficult-to-trace access to the monetary and benefits resources of the individual. The biometric identifier of an individual would be much more valuable. The greatly increased value of that information would make efforts to obtain it, efforts that may be seen as excessive now, quite worthwhile.

Final mention must be made of the danger to privacy that exists when a biometric tells more about an individual than who they are — providing much more than an accurate means of identification. DNA is the only biometric that currently falls into this group. The additional information about health and ethnic background, for example, that can be obtained from the DNA sample raises the danger to privacy significantly higher. An information system that knows your risk of hereditary disease (even when you don't) and which could be used to deny you access to health care or certain occupations must be regarded with particular concern. As stated above, the use of DNA is currently the only technology which can go beyond saying, "who you are" but new biometric technologies are constantly being developed. For example, the particular set of antibodies present in an individual's blood is being advanced as a possible unique identifier. With further development, this method could also be developed into a biometric technology that would not only identify an individual but would also include information on all the diseases to which the individual has been exposed.

5. Biometrics as a Friend to Privacy

There is, however, a counterpoint to the concern of the effects of biometric systems on privacy and perhaps a surprising one — biometrics can also be used to *protect* privacy. Identity theft is a real and growing fear, one that is posing an enormous problem in today's electronic society. No longer are we known to those we deal with day to day except through some representation of our identity. Our signature, a social benefits entitlement number, a credit card number, a PIN or a password all serve to identify us as we complete our transactions. But these identification measures can easily and fraudulently be taken away from us, often without our knowledge. And, once stolen, it is extremely difficult to recover one's true identity. The use of biometrics to establish and verify identity could securely safeguard that identity. Properly configured and maintained biometric systems are nearly impossible to fool. A virtually infallible identification measure that you carry at the end of your finger would be impossible to lose and close to impossible to fake.

The use of biometric systems to limit and monitor access to our information would also enhance our privacy. The restriction of unauthorized personnel from either physical or electronic access to databases of sensitive information safeguards that information. In addition, the transaction record provided by a biometric system would provide details on who entered a physical location or who accessed sensitive information.

A much greater step in using a biometric to protect privacy is through *biometric encryption*. Using this technology, the biometric is not itself the information that is stored. Rather, the biometric provides the key used to encrypt certain sensitive information. The technology of biometric encryption is new and has been developed around the use of a finger scan. Biometric encryption uses the unique pattern in a person's finger as one's private encryption or coding key to then scramble the data to be protected. The only way to unlock that data is to again present the matching (live) finger. The privacy protection afforded by such a system would truly make the use of such a biometric a friend of privacy.

6. Possible Legal Limitations on the Use of Biometric Information

The rights to privacy and fair information practices are part of the legal framework of most countries and come into play when dealing with any identification system like the biometrics technologies mentioned here. Additional legal limitations may exist with these systems depending on the jurisdiction. Prohibitions on unlawful search and seizure will undoubtedly have an impact. Obtaining a biometric record of an individual, particularly from a secondary source such as his or her employer, in the course of an investigation, could be seen as "search." How the jurisdiction's laws limit the process of "search" and whether there is an expectation of privacy within those laws could very well affect the legitimacy of obtaining a biometric record. Obtaining a biometric involuntarily, even if directly obtained from an individual, may be viewed as forced self-incrimination. A number of countries, Canada included, are either building or looking to build databanks of DNA information. The parameters of these systems, such as whether the information is obtained from those convicted of a particular set of crimes, those convicted of all crimes, or those only charged with a crime, will likely determine how the system is viewed in the context of due process protections of decency and fair play.

There are other, non-criminal, legal issues that may surround biometric systems. Labour laws in many jurisdictions limit the information that employers may require employees to provide. Privacy laws limit the disclosure of information to third parties for a purpose not consistent with the purpose of the original collection. Privacy laws may also restrict the merging of disparate databases. This would limit the ability to match biometric and other electronic information to develop a comprehensive profile about an individual. While exemptions to these limitations exist, particularly for law enforcement purposes, these laws will still need to be accommodated in the development of biometric systems. The portions of one law relating to the use of a biometric for the delivery of social assistance benefits, developed in Ontario, Canada, are included in the Appendix as one example of strong, legislated privacy protections in this area.

7. What Needs To Be Done To Make Partners of Biometrics and Privacy?

Whenever a balance between individual needs and societal needs must be struck, the development of legislation is perhaps the best way to achieve this balance. Although most Western jurisdictions have legislated privacy and information handling practices, there are some notable exceptions, with considerable variation in the laws. This means that separate legislation to cover the use of biometrics is called for. Public concerns about multi-purpose identification processes have been well documented and the unrestrained use of biometric technologies by disparate groups -- police, employers, social benefit administrators, etc., would undoubtedly meet with the same concerns. The use of biometrics needs to conform to the standards and expectations of a privacy-minded society.

At present, there is no universal requirement for people to identify themselves. In many countries, police have the power to demand that a person identify themselves only in particular circumstances or locations, such as when driving a motor vehicle. Widespread use of biometrics would change this if we are required to identify ourselves to enter buildings, use our computers, or conduct our banking activities. Secondary use of biometrics would shake the confidence of users in the technology. If you learned that your use of a biometric to secure access to your computer was also being used by your employer to record your time on the computer, for purposes of monitoring work performance without your knowledge, your feelings towards the universal benefits of biometrics would change.

Legislation, policies and procedures must be developed and conveyed to biometric users. When a biometric is to be collected, how it is used, to whom it is disclosed and how long it is retained must be clearly understood.

In addition, the unique identity of an individual as established by a biometric technology does not necessarily have to be linked to information that identifies an individual in society. In most biometric applications, once the identity of an individual is established, confirming that identity is all that is required to fulfill the purposes of the application. Use of anonymous or pseudonymous techniques could protect the privacy of the individual. To explain more fully, if the identity of an individual during initial enrollment into a biometric system is done using some anonymous label, the verification of that identity could take place each time the person used the system without being linked to the true identity of the individual. This is somewhat analogous to the use of passwords to access an individual computer. The first time you use that computer you are assumed by the computer to have permission to do so. Once you

set the password, the computer only knows at subsequent logons that you are the one authorized to use it but it does not need to know exactly who you are. If biometric systems took this approach, wherever possible, the public's view that these technologies were for their benefit (rather than to oversee their activities) would be greatly increased. Openness and transparency in the use of biometrics as with all other types of information systems, is a highly desirable goal to be sought after.

8. Conclusions

As in the case of most emerging technologies, biometrics has reached a crossroads in its development. The possibilities and benefits have been demonstrated, but before it moves into common usage, it is critical that its potential uses be examined to determine whether in each application, it is functioning as a friend or foe of privacy. Biometric systems do not necessarily have to be one or the other — they can be both. The use of biometrics to protect the privacy of the individual or to ensure the proper positioning of its use — so as not to jeopardize privacy, will mean not only that it receives a positive reception, but that it also fulfills its potential.

The policing community has two roles it can perform in this regard. First, it can control its own use of biometric information. The rights of the individual regarding identification have been firmly established in many areas. Just because those rights have not yet been as firmly established in the area of biometrics does not mean that the police should make use of them in ways that are inconsistent with the ways that they use any other identification method. In addition, the police have a role in guiding the non-policing community in their use of biometric technologies. Those inexperienced with using identification methods, be they employers, social benefit administrators or others, need guidance in the proper use of these powerful technologies. They will look to the policing community to guide them in a positive direction.

9. Appendix

Ontario Works Act, 1997 Statutes of Ontario, 1997, Chapter 25 Schedule A

Biometric information

75.(1) Where this Act or the regulations authorize a person to collect or use personal information, biometric information may be collected or used only for the following purposes:

1. To ensure that an individual is registered only once as an applicant, recipient, spouse or dependent adult.
2. To authenticate the identity of an individual who claims to be entitled to assistance.
3. To enable an individual to receive and give receipt for assistance provided through a financial institution or other authorized provider.
4. To enable an applicant, recipient, spouse or dependent adult to access personal information.
5. To enable an individual to make a declaration electronically by voice or other means for any purposes authorized under this Act.
6. To match data in accordance with an agreement made under section 71 or 72 for the purpose of ensuring eligibility for assistance or benefits.

75.(2) Biometric information may be collected under this Act only from the individual to whom it relates, in accordance with an agreement referred to in paragraph 6 of subsection (1) or in accordance with section 73.

75.(3) Biometric information shall not be disclosed to a third party except in accordance with,

(a) a court order or a warrant;

(b) an agreement under section 71 or 72 that is made for the purpose of ensuring eligibility for a social benefit program, including a social benefit program under the Income Tax Act or the Income Tax Act (Canada); or

(c) section 73.

75.(4) Biometric information to be collected from the individual to whom it relates shall be collected openly and directly from the individual.

75.(5) An administrator shall ensure that biometric information can be accessed and used only by those persons who need the information in order to perform their duties under this Act and that it is not used as a unique file identifier or common personal file identifier, except as authorized under subsection (1).

75.(6) An administrator shall ensure that biometric information collected under this Act is encrypted forthwith after collection, that the original biometric information is destroyed after encryption and that the encrypted biometric information is stored or transmitted only in encrypted form and destroyed in the prescribed manner.

75.(7) Neither the Director nor an administrator shall implement a system that can reconstruct or retain the original biometric sample from encrypted biometric information or that can compare it to a copy or reproduction of biometric information not obtained directly from the individual.

75.(8) The only personal information that may be retained together with biometric information concerning an individual is the individual's name, address, date of birth and sex.

75.(9) For the purpose of section 67 of the Freedom of Information and Protection of Privacy Act and section 53 of the Municipal Freedom of Information and Protection of Privacy Act, subsection (3) is a confidentiality provision that prevails over those Acts. 1997, c. 25, Sched. A, s. 75.

76.(1) Electronic signature

76.(1) Where this Act or the regulations require an individual's signature, one or more of the individual's personal identification number (PIN), password, biometric information or photographic image may be used in the place of his or her signature to authenticate the individual's identity and to act as authorization of or consent to a transaction relating to an application for or the receipt of assistance.

76.(2) If a person collects an individual's personal identification number (PIN), password, biometric information or photographic image under this Act, it shall be recorded and stored in a secure electronic environment. 1997, c. 25, Sched.. A, s. 76.

77.(1) No personal liability

77.(1) No action or other proceeding in damages shall be instituted against the Ministry, the Director, a delivery agent, an officer or employee of any of them or anyone acting under their authority for any act done in good faith in the execution or intended execution of a duty or authority under this Act or for any alleged neglect or default in the execution in good faith of any duty or authority under this Act.

77.(2) Liability of Crown

77.(2) Subsection (1) does not, by reason of subsections 5 (2) and (4) of the Proceedings Against the Crown Act, relieve the Crown of liability in respect of a tort committed by a person mentioned in subsection (1) to which it would otherwise be subject. 1997, c. 25, Sched. A, s. 77.

78. Penalty

78. If a delivery agent fails to properly exercise a power or duty under this Act or the regulations, the Minister may deduct from the amount payable by Ontario a portion of the delivery agent's share of the cost of administering this Act and providing assistance, in accordance with the regulations. 1997, c. 25, Sched. A, s. 78.

79.(1) Offence

79.(1) No person shall knowingly obtain or receive assistance to which he or she is not entitled under this Act and the regulations.

79.(2) No person shall knowingly aid or abet another person to obtain or receive assistance to which the other person is not entitled under this Act and the regulations.

79.(3) Obstruction

79.(3) No person shall obstruct or knowingly give false information to a person engaged in investigations for the purposes of section 57 or 58.

79.(4) Penalty

79.(4) A person who contravenes subsection (1), (2) or (3) is guilty of an offence and on conviction is liable to a fine of not more than $5,000 or to imprisonment for a term of not more than six months or to both. 1997, c. 25, Sched. A, s. 79.

10. Bibliography

Cavoukian, Ann, Ph.D. and Tapscott, Don; *Who Knows: Safeguarding Your Privacy in a Networked World*, McGraw-Hill: New York, 1997.

Clarke, Roger, Human Identification in Information Systems: Management Challenges and Public Policy Issues; *Information Technology & People*, Vol. 7, No. 4, 1994.

Davies, Simon G., Touching Big Brother: How biometric technology will fuse flesh and machine; *Information Technology & People*, Vol. 7, No. 4, 1994.

O'Connor, Sean M., Collected, Tagged, and Archived: Legal Issues in the Burgeoning Use of Biometrics for Personal Identification: http://lummi.stanford.edu/class/law495/WWW/oconnor.htm

Roethenbaugh, Gary, Biometrics Explained: http://www.icsa.net/services/consortia/cbdc/explained.shtml

Tomko, George, Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?, Privacy Laws and Business 9th Privacy Commissioners'/Data Protection Workshop, 1998: http://www.dss.state.ct.us/digital/tomko.htm

Woodward, John D., Biometrics: Privacy's Foe or Privacy's Friend? Proceedings of the IEEE, September 1997.